PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-047987
(43)Date of publication of application : 18.02.2000

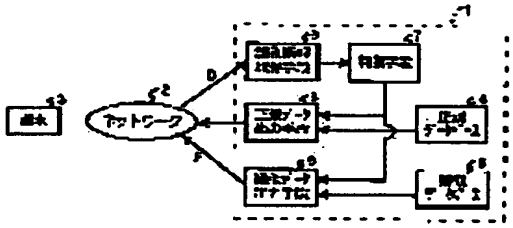
(51)Int.CI. G06F 15/00
H04L 9/32
// G06F 17/30

(21)Application number : 10-214983
(22)Date of filing : 30.07.1998

(71)Applicant : FUJI PHOTO FILM CO LTD
(72)Inventor : NAKAMURA ATSUSHI
ITO WATARU

(54) METHOD AND DEVICE FOR OUTPUTTING DATA, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent data from flowing to a person illegally accessing a data base or the like.
SOLUTION: A judging means 7 judges whether identification information D acquired from a terminal 3 is regular or not. When it is regular, regular data T are read out of a regular data base 4 and the regular data T are outputted from a regular data output means 8 to the terminal 3. When the identification information D is not regular, dummy data F similar to the regular data T but different from them are read out of a dummy data base 5 and the dummy data F are outputted from a dummy data output means 9 to the terminal 3. Thus, even in the case of illegal access, since any data are acquired at the terminal 3, the illegally accessing person has the illusion of making the access successful.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－47987
（P2000－47987A）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０７５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７１	５Ｂ０８５
// Ｇ０６Ｆ　17/30		Ｇ０６Ｆ　15/40	３２０Ｚ	５Ｋ０１３

審査請求　未請求　請求項の数15　ＯＬ　（全７頁）

(21)出願番号　特願平10－214983

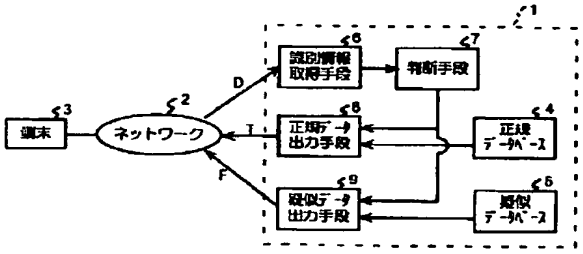
(22)出願日　平成10年７月30日(1998.7.30)

(71)出願人　000005201
富士写真フイルム株式会社
神奈川県南足柄市中沼210番地
(72)発明者　中村　淳
神奈川県足柄上郡開成町宮台798番地　富士写真フイルム株式会社内
(72)発明者　伊藤　渡
神奈川県足柄上郡開成町宮台798番地　富士写真フイルム株式会社内
(74)代理人　100073184
弁理士　柳田　征史　（外１名）

Ｆターム(参考)　5B075 KK43 KK54 KK63 ND02 PQ12
5B085 AC03 AE01 AE06
5K013 GA02

(54)【発明の名称】　データ出力方法および装置並びに記録媒体

(57)【要約】
【課題】　データベース等への不正アクセス者に対するデータの流出を防止する。
【解決手段】　端末３から取得した識別情報Ｄが正規のものであるか否かを判断手段７において判断する。正規のもである場合には、正規データベース４から正規データＴを読み出し、正規データ出力手段８より正規データＴを端末３に出力する。識別情報Ｄが正規のものでない場合には、正規データＴとは似て非なる疑似データＦを疑似データベース５から読み出し、疑似データ出力手段９より疑似データＦを端末３に出力する。これにより、不正アクセスの場合でも、何らかのデータが端末３において取得されるため、不正アクセス者に対してアクセスに成功したかのような錯覚を起こさせることができる。



1

【特許請求の範囲】

【請求項１】　データを取得するための識別情報の取得に基づいて、前記識別情報に対応する正規データの出力を許容するか否かを判断し、前記正規データを出力することが許容された場合に、該正規データを出力するデータ出力方法において、

前記正規データを出力することが許容されなかった場合に、前記正規データとは異なる疑似データを出力することを特徴とするデータ出力方法。

【請求項２】　前記疑似データを、該疑似データを蓄積する疑似データ蓄積手段から出力することを特徴とする請求項１記載のデータ出力方法。

【請求項３】　前記疑似データを前記正規データに基づいて作成することを特徴とする請求項１記載のデータ出力方法。

【請求項４】　前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データであることを特徴とする請求項１から３のいずれか１項記載のデータ出力方法。

【請求項５】　前記取得された識別情報を所定形式の比較識別情報と比較し、

前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止することを特徴とする請求項１から４のいずれか１項記載のデータ出力方法。

【請求項６】　正規データを蓄積した正規データ蓄積手段と、

前記正規データを取得するための識別情報を取得する識別情報取得手段と、

該識別情報取得手段により取得された前記識別情報に基づいて、該識別情報に対応する正規データの出力を許容するか否かを判断する判断手段と、

該判断手段により前記正規データを出力することが許容された場合に、該正規データを出力する正規データ出力手段とを備えたデータ出力装置において、

前記判断手段により前記正規データを出力することが許容されなかった場合に、前記正規データとは異なる疑似データを出力する疑似データ出力手段をさらに備えたことを特徴とするデータ出力装置。

【請求項７】　前記疑似データを蓄積する疑似データ蓄積手段をさらに備えたことを特徴とする請求項６記載のデータ出力装置。

【請求項８】　前記正規データに基づいて前記疑似データを作成する疑似データ作成手段をさらに備えたことを特徴とする請求項６記載のデータ出力装置。

【請求項９】　前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データであることを特徴とする請求項６から８のいずれか１項記載のデータ出力装置。

【請求項１０】　前記入力された識別情報を所定形式の

2

比較識別情報と比較する比較手段と、

前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止する禁止手段とをさらに備えたことを特徴とする請求項６から９のいずれか１項記載のデータ出力装置。

【請求項１１】　データを取得するための識別情報の取得に基づいて、前記識別情報に対応する正規データの出力を許容するか否かを判断し、前記正規データを出力することが許容された場合に、該正規データを出力するデータ出力方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体において、

前記プログラムは、前記正規データを出力することが許容されなかった場合に、前記正規データとは異なる疑似データを出力する手順を有することを特徴とするコンピュータ読取り可能な記録媒体。

【請求項１２】　前記疑似データを出力する手順は、前記疑似データを、該疑似データを蓄積する疑似データ蓄積手段から出力する手順であることを特徴とする請求項１１記載のコンピュータ読取り可能な記録媒体。

【請求項１３】　前記疑似データを前記正規データに基づいて作成する手順をさらに有することを特徴とする請求項１１記載のコンピュータ読取り可能な記録媒体。

【請求項１４】　前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データであることを特徴とする請求項１１から１３のいずれか１項記載のコンピュータ読取り可能な記録媒体。

【請求項１５】　前記取得された識別情報を所定形式の比較識別情報と比較する手順と、

前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止する手順とをさらに有することを特徴とする請求項１１から１４のいずれか１項記載のコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＤ等の識別情報を取得し、この識別情報に基づいてデータを出力するデータ出力方法および装置並びにデータ出力方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体に関するものである。

【０００２】

【従来の技術】近年、ネットワークを介して種々のデータのやり取りが行われている。このようにネットワークを介してやり取りされるデータには、機密度の高いもの、個人的なデータ、著作権により保護されるべきデータ等が含まれている。したがって、これらのデータを暗号化したり、キーワードを用いたりする等して、特定の者以外の不正アクセス者によるデータへのアクセスを禁

止することにより、これらのデータを不正な利用から保護する必要がある。このようなデータ保護の方式としては、例えば、電子化された画像データに暗号化情報を埋め込む方式（特開平５－２３６４２４号）、媒体に固有番号を付与し、この媒体固有番号に対してのみソフトウエアの実行を許可する方式（特開平５－２５７８１６号）、共通鍵を用いる方式において、共通鍵により暗号化された情報本体と利用条件情報とを別の記憶部に記憶しておき、情報の改竄を検出する方式（特開平７－１３１４５２号）等が知られている。これらの方式は、暗号、キーワード、固有番号等が一致しない場合には、データの表示や提供を禁止するものであり、不正なアクセスを行った者に対してアクセスが失敗したことを告知するものである。

【０００３】

【発明が解決しようとする課題】しかしながら、これらの方式においては、暗号やキーワードを何回も入力し直すことにより、いずれは暗号やキーワードが解読されるおそれがあり、その結果データが不正アクセス者に流出するおそれがある。

【０００４】本発明は上記事情に鑑みなされたものであり、不正アクセス者に対するデータの流出を防止できるデータ出力方法および装置並びにデータ出力方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体を提供することを目的とするものである。

【０００５】

【課題を解決するための手段】本発明によるデータ出力方法は、データを取得するための識別情報の取得に基づいて、前記識別情報に対応する正規データの出力を許容するか否かを判断し、前記正規データを出力することが許容された場合に、該正規データを出力するデータ出力方法において、前記正規データを出力することが許容されなかった場合に、前記正規データとは異なる疑似データを出力することを特徴とするものである。

【０００６】ここで、「疑似データ」とは、正規データと似て非なるデータのように、不正アクセス者がアクセスに失敗したことを自覚しない程度のデータのことをいい、例えば画像データの場合は正規データのように見えるが正規データにより表される画像と類似した色調あるいは類似した構図の画像を表す画像データ、数値を配列したデータの場合はその数値の並び方、数値の内容、桁数、データ形式等を変更したデータのことをいう。

【０００７】また、「識別情報を取得する」とは、アクセス者が自ら識別情報を入力する場合の他、アクセスされた端末の端末ＩＤを自動的に取得する、あるいは電話回線を使用してアクセスされた場合には端末の電話番号を自動的に取得する場合をも含むものである。

【０００８】なお、前記疑似データを、該疑似データを蓄積する疑似データ蓄積手段から出力するようにしてもよく、前記疑似データを前記正規データに基づいて作成するようにしてもよい。

【０００９】また、前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データとすることが好ましい。

【００１０】さらに、前記取得された識別情報を所定形式の比較識別情報と比較し、前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止することが好ましい。

【００１１】本発明によるデータ出力装置は、正規データを蓄積した正規データ蓄積手段と、前記正規データを取得するための識別情報を取得する識別情報取得手段と、該識別情報取得手段により取得された前記識別情報に基づいて、該識別情報に対応する正規データの出力を許容するか否かを判断する判断手段と、該判断手段により前記正規データを出力することが許容された場合に、該正規データを出力する正規データ出力手段とを備えたデータ出力装置において、前記判断手段により前記正規データを出力することが許容されなかった場合に、前記正規データとは異なる疑似データを出力する疑似データ出力手段をさらに備えたことを特徴とするものである。

【００１２】なお、前記疑似データを蓄積する疑似データ蓄積手段をさらに備えるようにしてもよく、前記正規データに基づいて前記疑似データを作成する疑似データ作成手段をさらに備えるようにしてもよい。

【００１３】また、前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データであることが好ましい。

【００１４】さらに、前記入力された識別情報を所定形式の比較識別情報と比較する比較手段と、前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止する禁止手段とをさらに備えることが好ましい。

【００１５】なお、本発明によるデータ出力方法をコンピュータに実行させるプログラムとして、コンピュータ読取り可能な記録媒体に記録して提供してもよい。

【００１６】

【発明の効果】本発明によれば、正規データを出力することが許容されなかった場合に、正規データに対応する疑似データを出力するようにしたため、不正アクセス者をあたかもアクセスに成功して正規データを入手したかのような錯覚に陥らせることができる。したがって、不正アクセス者にアクセス失敗を悟られることがなくなり、これにより正規データの不正な流出や、識別情報の解析等の不正行為を防止することができる。

【００１７】また、取得した識別情報を所定形式の比較識別情報と比較し、識別情報が比較識別情報と異なる場合には、正規データおよび疑似データの出力を禁止する

ことにより、何回かアクセスに失敗した不正アクセス者が比較識別情報の形式と同一形式の識別情報を入力した際に疑似データが出力されることとなるため、不正アクセス者に対してあたかもアクセスに成功したかのように勘違いさせることが可能となる。

【００１８】

【発明の実施の形態】以下図面を参照して本発明の実施形態について説明する。

【００１９】図１は本発明の第１の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図である。図１に示すように、このデータ出力システムは、本実施形態によるデータ出力装置１と、このデータ出力装置１にネットワーク２を介して接続された端末３とからなる。

【００２０】データ出力装置１は、正規データＴを蓄積した正規データベース４と、疑似データＦを蓄積した疑似データベース５と、端末３から入力された識別情報Ｄを取得する識別情報取得手段６と、識別情報取得手段６により取得された識別情報Ｄに基づいて、識別情報Ｄに対応する正規データＴの出力を許容するか否かを判断する判断手段７と、判断手段７により正規データＴを出力することが許容された場合に、正規データＴを端末３に出力する正規データ出力手段８と、判断手段７により正規データＴを出力することが許容されなかった場合に、疑似データＦを端末３に出力する疑似データ出力手段９とを備える。

【００２１】判断手段７は、取得した識別情報Ｄが正規の識別情報であるか否かを判断し、識別情報Ｄが正規のものであると判断された場合に、この識別情報Ｄに対応する正規データＴを正規データベース４から読み出して正規データ出力手段８によりネットワーク２を介して端末３に出力する。一方、取得した識別情報Ｄが正規のものでないと判断された場合には、この正規データＴに対応する疑似データＦを疑似データベース５から読み出して疑似データ出力手段９によりネットワーク２を介して端末３に出力する。

【００２２】ここで、識別情報Ｄとしては、暗証番号、キーワード等端末３のアクセス者が端末３に設けられたキーボード等の入力手段から直接入力するものの他、端末３のＩＤや電話回線を介してアクセスがあった場合には、端末３の電話番号等、自動的に取得されるものをも含む。

【００２３】また、疑似データＦとしては例えば正規データＴが図２に示すような数値データである場合には、図３に示すように数値を並び替えたデータを用いる。このように、数値を並び替えた場合その合計値を並び替えた数値に対応させることにより、疑似データＦをより正規データＴらしく見せることができる。また、正規データＴの数値の内容、桁数、データ形式を変更したものを疑似データＦとしてもよい。なお、正規データＴが画像データである場合には、疑似データＦを正規データＴのように見えるが正規データＴにより表される画像と類似した色調あるいは類似した構図の画像を表す画像データ等とすればよい。

【００２４】次いで、第１の実施形態の動作について説明する。図４は第１の実施形態の動作を示すフローチャートである。まず、識別情報取得手段６において端末３から識別情報Ｄを取得する（ステップＳ１）。次に判断手段７において、取得した識別情報Ｄが正規のものであるか否かが判断される（ステップＳ２）。識別情報Ｄが正規のものである場合にはステップＳ２が肯定され、正規データベース４から識別情報Ｄに対応する正規データＴを読み出し、正規データ出力手段８からネットワーク２を介して端末３に正規データＴを出力する（ステップＳ４）。この場合、端末３の利用者は正規のアクセス者であることから、端末３においてはアクセス者が所望とする正規データＴを得ることができる。

【００２５】一方、識別情報Ｄが正規のものでない場合にはステップＳ２が否定され、疑似データベース５から疑似データＦを読み出し、疑似データ出力手段９からネットワーク２を介して端末３に疑似データＦを出力する（ステップＳ３）。この場合、端末３の利用者は不正アクセス者であることから、端末３においてはあたかもアクセスに成功したかのように疑似データＦが得られる。

【００２６】このように第１の実施形態によれば、不正アクセスがあった場合に、正規データＴに対応する疑似データＦを出力するようにしたため、不正アクセス者をあたかもアクセスに成功して正規データＴを入手したかのような錯覚に陥らせることができる。したがって、不正アクセス者にアクセス失敗を悟られることがなくなり、これにより正規データＴの不正な流出や、識別情報Ｄの解析等の不正行為を防止することができる。

【００２７】なお、第１の実施形態においては、不正アクセスがあった場合に、疑似データベース５から疑似データＦを読み出して端末３に出力しているが、図５に示す第２の実施形態のように、疑似データベース５に代えて、正規データＴから疑似データＦを作成する疑似データ作成手段１０を備えるようにしてもよい。第２の実施形態においては、不正なアクセスがあった場合に、正規データベース４から正規データＴを読み出し、この正規データＴに基づいて疑似データ作成手段１０において疑似データＦを作成し、作成された疑似データＦが疑似データ出力手段９よりネットワーク２を介して端末３に出力されることとなる。

【００２８】次いで、本発明の第３の実施形態について説明する。図６は本発明の第３の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図である。第３の実施形態は、判断手段７にて識別情報Ｄが予め登録された所定の形式であるか否かを判断し、所定の形式でありかつ正規の識別情報Ｄであ

る場合には正規データＴを出力し、所定の形式でありかつ正規の識別情報Ｄでない場合には疑似データＦを出力し、所定の形式でない場合には正規データおよび疑似データを出力することなくアクセスに失敗した旨を表すデータＰを出力するようにした点が第１の実施形態と異なるものである。そして、第３の実施形態においては、このアクセスに失敗した旨を表すデータＰを出力する出力禁止手段１１を備えてなるものである。

【００２９】第３の実施形態の判断手段７においては、図７（ａ）に示すような複数のダミーＩＤおよび図７（ｂ）に示す真の登録ＩＤが登録されている。本実施形態においては、判断手段７においてアクセスしている端末３のＩＤが判断され、その端末ＩＤが正規のものである場合に、アクセス者が入力した識別情報Ｄが登録ＩＤと比較される。ここで、本実施形態においては、複数の誕生日形式のダミーＩＤを登録しておき、登録されたダミーＩＤと同一形式の識別情報Ｄが入力された時にダミーＩＤと一致し、それ以外の形式の識別情報Ｄが入力された時にダミーＩＤと一致しないと判断するものである。

【００３０】出力禁止手段１１は、判断手段７による判断結果が登録ダミーＩＤと一致しないものである場合に、例えば「アクセス失敗」の表示を端末３で行うようなデータＰをネットワーク２を介して端末３に出力するものである。

【００３１】次いで、第３の実施形態の動作について説明する。図８は第３の実施形態の動作を示すフローチャートである。まず、識別情報取得手段６において端末３の識別情報Ｄおよびアクセスしている端末３の端末ＩＤを取得する（ステップＳ１１）。次に判断手段７において、取得した端末ＩＤが正規の端末ＩＤと一致するか否かが判断される（ステップＳ１２）。取得した端末ＩＤが正規の端末ＩＤと一致する場合はステップＳ１２が肯定され、さらに取得した識別情報Ｄが正規のものであるか否かが判断される（ステップＳ１３）。識別情報Ｄが正規のものである場合には、正規データベース４から識別情報Ｄに対応する正規データＴを読み出し、正規データ出力手段８からネットワーク２を介して端末３に正規データＴを出力する（ステップＳ１６）。この場合、端末３の利用者は正規のアクセス者であることから、端末３においてはアクセス者が所望とする正規データＴを得ることができる。

【００３２】一方、識別情報Ｄが正規のものでない場合にはステップＳ１３が否定され、さらにステップＳ１４において、識別情報Ｄが登録されたダミーＩＤと一致するか否かが判断される。識別情報ＤがダミーＩＤと一致する場合は疑似データベース５から疑似データＦを読み出し、疑似データ出力手段９からネットワーク２を介して端末３に疑似データＦを出力する（ステップＳ１５）。この場合、端末３の利用者は不正アクセス者であることから、端末３においてはあたかもアクセスに成功したかのような疑似データＦが得られる。なお、ステップＳ１２において端末ＩＤが正規の端末ＩＤでないと判断された場合にも、ステップＳ１５において疑似データＦが出力される。

【００３３】さらに、識別情報ＤがダミーＩＤと一致しない場合には、正規データＴおよび疑似データＦの出力を禁止するとともに、出力禁止手段１１からネットワーク２を介して端末３にデータＰを出力する（ステップＳ１７）。この場合、端末３にはアクセス失敗の旨の表示がなされることとなる。

【００３４】このように第３の実施形態によれば、識別情報ＤをダミーＩＤと比較し、識別情報Ｄがダミーと異なる場合には、正規データＴおよび疑似データＦの出力を禁止するとともに、アクセス失敗の旨を表すデータＰを出力するようにしたため、何回かアクセスに失敗した不正アクセス者がダミーＩＤと同一形式の識別情報Ｄを入力した際には疑似データＦが出力されることとなり、その結果、不正アクセス者に対してあたかもアクセスに成功したかのように勘違いさせることが可能となる。

【００３５】なお、上記第３の実施形態においては、疑似データベース５から疑似データＦを読み出して端末３に出力しているが、第２の実施形態のように、正規データＴから疑似データＦを作成するようにしてもよい。

【００３６】また、上記第３の実施形態においては、ダミーＩＤを誕生日の形式としているが、これに限定されるものではなく、電話番号等任意の形式としてもよい。さらに、登録されたダミーＩＤと一致するか否かを判断しているが、例えば識別状Ｄの桁数が予め登録した桁数と一致するか否かを判断するようにしてもよい。

【００３７】さらに、上記第３の実施形態においては、ステップＳ１２において端末ＩＤが正規の端末ＩＤでないと判断された場合に、ステップＳ１５において疑似データＦを出力しているが、ステップＳ１７と同様に、正規データＴおよび疑似データＦの出力を禁止するとともにデータＰを出力し、端末３においてアクセス失敗の旨を表示するようにしてもよい。

【００３８】なお、上記各実施形態においては、端末３における正規のアクセス者が本当に正規データＴを取得したか否かが分からなくなるおそれがある。したがって、正規データＴを出力した後、利用者の登録住所への輸送、電話あるいはＥメール等により、正規データＴを出力した旨の立証をすることが好ましい。

【図面の簡単な説明】

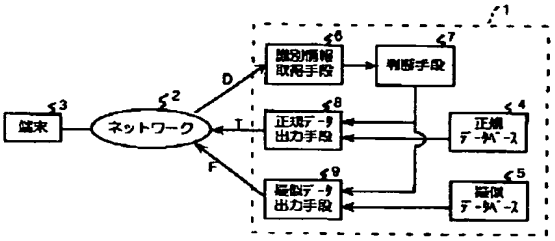
【図１】本発明の第１の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図

【図２】正規データの例を示す図

【図３】疑似データの例を示す図

【図４】第１の実施形態の動作を示すフローチャート
【図５】本発明の第２の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図
【図６】本発明の第３の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図
【図７】ダミーＩＤおよび真の登録ＩＤを示す図
【図８】第３の実施形態の動作を示すフローチャート
【符号の説明】
1　　データ出力装置
＊2　　ネットワーク
3　　端末
4　　正規データベース
5　　疑似データベース
6　　識別情報取得手段
7　　判断手段
8　　正規データ出力手段
9　　疑似データ出力手段
１０　疑似データ作成手段
１１　出力禁止手段

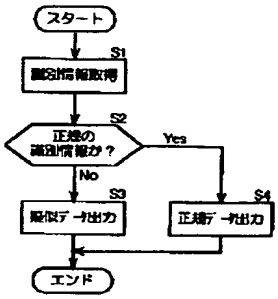
【図１】



【図２】

	A店	B店	C店	合計
1月度	123	456	789	1368
2月度	234	567	123	924
3月度	564	156	389	1109
合計	921	1179	1301	3401

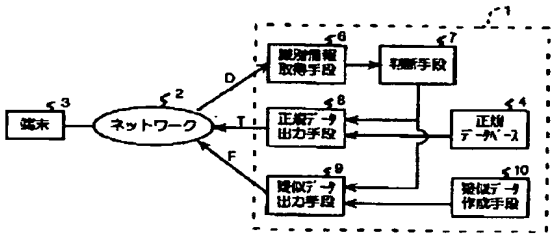
【図４】



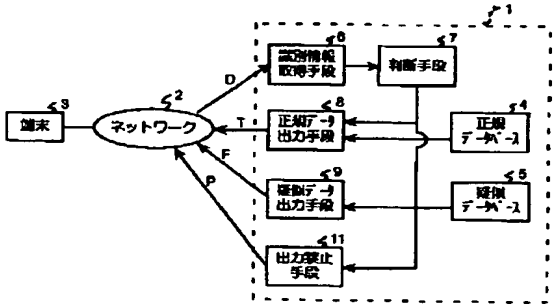
【図３】

	A店	B店	C店	合計
1月度	567	789	123	1479
2月度	123	456	156	735
3月度	789	389	564	1742
合計	1479	1634	843	3956

【図５】



【図６】



【図７】

(a)

```
登録ダミーＩＤ
  端末ＩＤ　AA12345
    760521　870421
    680118　640301
    ……
  端末ＩＤ　AA12346
    460221　771212
    881207　811030
    ……
```

(b)

```
真の登録ＩＤ
  端末ＩＤ　AA12345：590382，…
  端末ＩＤ　AA12346：771111，…
```

【図８】